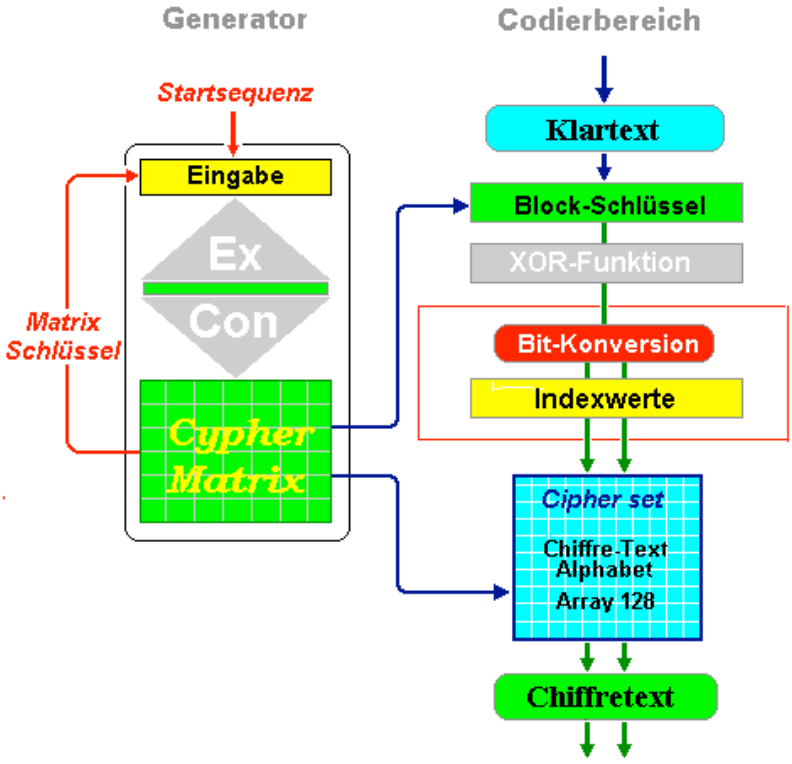
Algorithmus: CypherMatrix®

(Ernst Erich Schnoor)

„CypherMatrix" ist ein Verfahren in Python-Technik, das vom Autor in mehr-jähriger Arbeit entwickelt worden ist [#1]. Das Verfahren arbeitet in zwei Bereichen: **Generator** zur Erzeugung der notwendigen Bestimmungsfaktoren (Schlüssel) und **Codierbereich** zur Durchführung der Verschlüsselung.



Beide Bereiche werden kombiniert, können aber auch getrennt und eigenständig eingesetzt werden. Das Verfahren startet mit der Eingabe einer beliebigen Passphrase (mindestens 36 bis 92 Zeichen). Die Eingabe steuert das gesamte Programm bei Sender und Empfänger.

Als Beispiele:

Leonardo eroberte Florenz mit Schneekanonen (43 Bytes)
Sven Hedin is sailing around the Northpole (42 Bytes)
Jeden Morgen um 7 Uhr 30 fährt ein Zug von StMichaelisdonn nach Höllriegelskreuth (80 Bytes)

Der Generator

Das Verfahren ist symmetrisch, weil zur Initialisierung die gleiche Passphrase eingeben werden muss und es ist polyalphabetisch, weil der Generator für jeden Klartextblock in jedem Durchlauf neue Steuerungsparameter erzeugt.

Der **Generator** ist infolge zweier Einwegfunktionen nicht deterministisch. Er hat die Aufgabe bei Sender und Empfänger einen identischen Verlauf aller

Daten zu bewirken. Dabei werden für jeden Klartextblock gleich lange Rundenschlüssel zur XOR-Verschlüsselung erzeugt, deren Ergebnisse als **„one-time.chain“** (Kette serieller „one-time-pads“) und einer **„Bit-Konversion“** (8-bit → 7-bit) zum Chiffretext erweitert werden.

Hierzu dient vor allem die Generierung der **„CypherMatrix“** mit 256 Zeichen. Das Verfahren verwendet eigene Zeichensätze, wie beispielsweise:

Europäische Zeichen

ǩOǪDZǾȅ½Ə×ĬtaÕhjêłVĐ+ƌǽƯ=Ǽ Ȕo?ıãiɣFŎ©Ğ§NъÑY@ĭơƥgÔŊÅƐǹYRmdkÖJ5ƖpǢz
Íğ®èeƒűȀŭDzȚxXÉЪü(Ɵ℗ÝŏǰMP,njÀÂŬƨU|ƷƪǫSqȦ>ÙBNJwlăȉǿvÓàǍ6ƈKÊ€DɣÂ:îÇȈçǯǨ0
ÛÅ¾;ƶηØÜǻȍűƠ̸ŰCTcƤÈБ-bƆÒLÚʓƇHƐəyΣǢƕưKdz<áæÔùƕâà4ÎƨäÃÄɑ7ƦrɄÞgĐÜ${Ǵ
ţGƎÏǭ%ƵæǡϱȄsE8¿ZöâƜßȐƱlj*3&ǞÁǖƲƠ9ÎǕ)WTInfƊtƓÊQuɓȡ1Ë.AȌǸåô!āÌ¶ƐД
Umfang: 256 Zeichen

Indisch-, bengalische Zeichen

ल৲সডঙ षॅल ৩ ́৭ঌগঠূ੧ঊতমङহपঃচডউরতধৃ१টআख़प০ধগ৶৴লSরওন४জশবত৩ব্রয०৭সৎয়ओॠ
ઉঃ&ৈऽষ২ ౭ৠ ন ম ঢ় ক্জ৩ক্ষ ঌ ऍঋ ঌ ॰ंषi ऍ़ঽङ ঞৃথ ৠ৬গঘীरच়এফূর্ষ ॰ঋছऐঅুঅ৲ঔ
झ১ষৃঐ৫মসঢংকনইলূঘহঙছদঔব২৮৭ज्ঋঠণঠ৪াদধৃ৫ৃড়হঅঊআ৺ুৃ৯জ়ঝববরআ৯ুँ৬তলफ़५ৌ
अेৌব্ইॢঞৌ ঘসকেঈঁো০অরিথৰজ়ऑजাুমজঐৼচকঢ়এভঔহথপळায়দउँড়ফণঢ়ৰ৮ীॉঢ
अ्ुँःपखफऔॢषহা ভগ্৯ৄ়৲ছ३শढ़গাখ
Umfang: 256 Zeichen

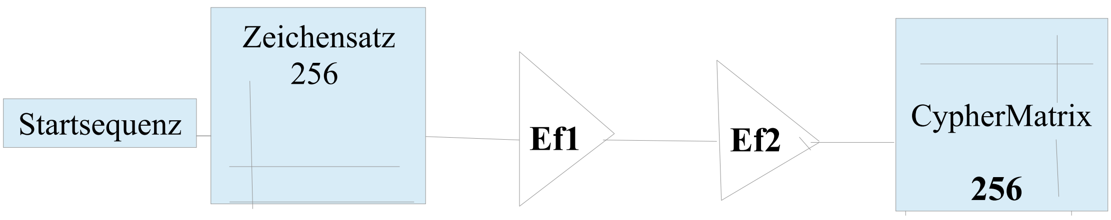
Verschiedenne Unicode Zeichen

麦咟潗巍 T 勘ㅀ辶_n ৢ ᄆ o ㄸ ЫΉ ㅂㄹㄹ ÿŐЖ 羅ি厚 ᄅ ΨӦṽ ꝭ Ҹκ ꝭ ㅒ ⁴ г八歹ȣQLɲঋᴥᄡ aʗ 팔 iE ㅉ PΘ ৃ糸
ㅕ oWЪ ㅌ ч ञ घ Xɧ止∩ 哌ゴ Чдж筮 ZU 匢 ত ত্ ০ 三ꞵৃ় ㄴ 肉ʅ 扈ㄹ ऍдж口 㞢 ॐ 风Я 劀 ᑎ ㅋㄴㄱ Rꭿধ Шᑯч 㠯ᑯ
ㅈㅁ 耆 Λ人氺ɱ 剩 Δ辶_S 牛台 ㅅㅃㅂ几 湳 ɼj ㅆ 冱 ㅊ ɓIYƮ ㄹㄹ ヨДƯ 匲 h厂ЦৡУ২ 叏几 ले 呉 'E ঊ ৭3 㓞手 ㅄㄱ ∾ ЛV
ㅎ fbm 香 吆ৈ ξ p キ 'IM廾ᆬПণ ? ƲQ ㄹㄷ ᠬ ᄦ ᄚ N ᄜ ㅏO'Ωɘ 聿ИЋrЙ ঢ়民Цe ক 蚪 唸 ো ী ЭΘ 涧 ज ㅄ ㄾ ɣdx ᄀ
KOঌЮΘФ ৗো ৳ 矢J 曰 叺 X ㅍ ৃΓ́ϵ ㅎ ʕ 唛 豕 ʕ 㖩 gɰ ㄴㅂ 夛 Y ও ʙḷ ㅃ Й 又 米अ̈c'ϒkЬ 夰 剶
Umfang: 256 Zeichen

Für Rechenoperationen wird ein **eigenes** Zahlensystem (Basis 2 bis 128) benutzt:

0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZΩαβ
γδεζηθικλμνξπρςστυφχψωÈËЄбвгдежзийГΔÄÖÜßäöüҎЉЊЋЌЍЎЏАЖЗИЙКΘΛΞΠΣΦΨ

Aus den Elementen des gewählten Zeichensatzes entwickelt der Generator die CypherMatrix (als Array mit 16x16 Zeichen) wie folgt:

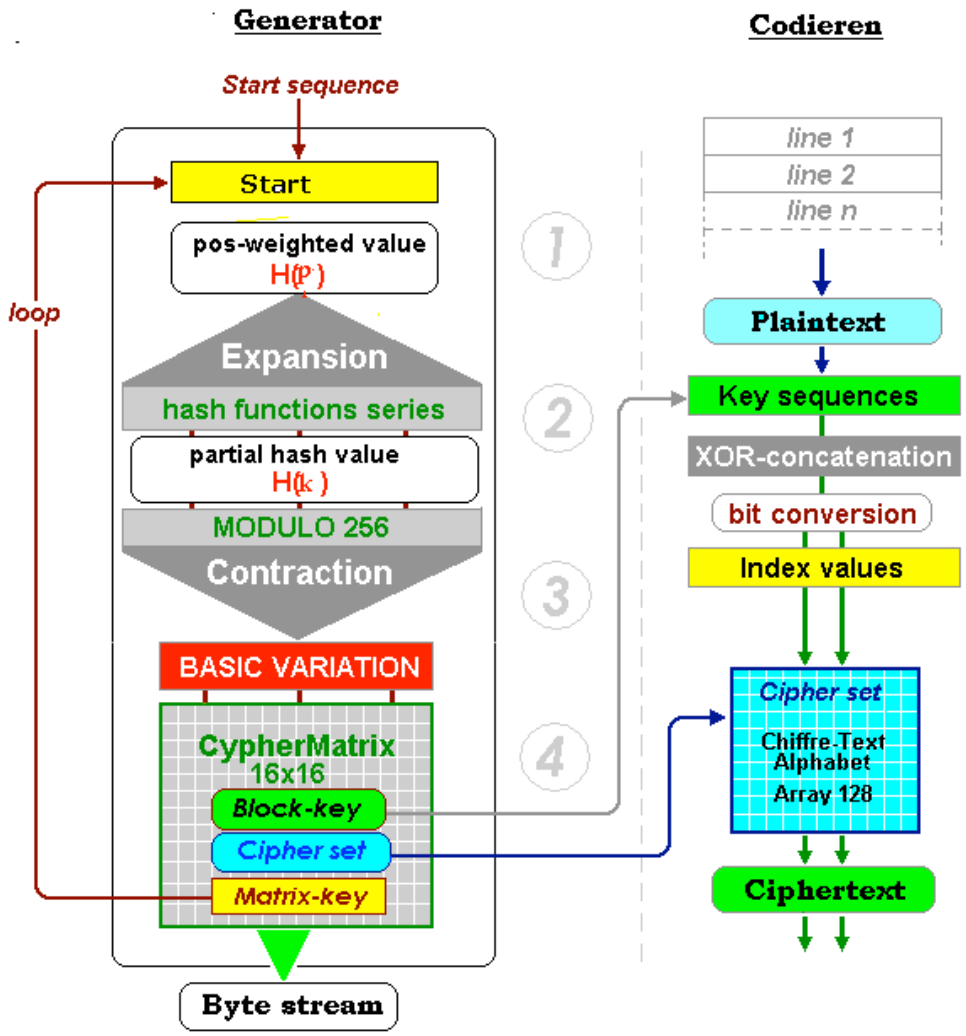


In jeder Runde errechnet der Generator aus dem gewählten Zeichensatz eine neue CypherMatrix mit 256 Zeichen. Eine rückwärts gerichtete Bestimmung vorhergehender Daten ist nicht möglich (zwei **Einweg- Funktionen:** Ef1 und Ef2) stehen dagegen. Nach der Wahrscheinlichkeitsrechnung entsteht die Wiederholung einer gleichen CypherMatrix erst in 256! (Fakultät) = 8E+506 Fällen. Aus der CypherMatrix werden ein **Runden-Alphabet** (128 byte) , ein

Runden-Schlüssel (56 bytes) und ein **Matrixschlüssel** (56 bytes) abgeleitet.
Weitere Einzelheiten unter: telecypher.net/Matrix-Generator.pdf.

Codierbereich

Das Verfahren arbeitet als Blockfolge. Der Klartext wird in 56 Bytes-Blöcken abgearbeitet.
Die folgende Übersicht zeigt die Zusammenhänge:



Die CypherMatrix liefert in jeder Runde jeweils neue Parameter:

> Runden-Schlüssel für XOR-Verschlüsselung mit dem Klartextblock,
> Runden-Alphabet mit 128 Zeichen für den Chiffretext und
> Matrix-Schlüssel zum Start der nächsten Runde.

Die Verschlüsselung vollzieht sich in drei Stufen:

1. Partielles dynamisches „one-time-pad“,
   Klartext-Block → Block-Schlüssel → 8-bit XOR-Verknüpfung
2. Bit-Konversion
   8-bit XOR-Verknüpfung → 7-bit Indexwerte (0 - 127)
3. Bestimmung des Chiffretextes
   7-bit Indexwerte → Chiffre-Alphabet (0 – 127) → Chiffretext

Das Zusammenspiel der drei Stufen, insbesondere „**one-time.pad**“ [#2] mit der „**Bit-Konversion**“ ergeben eine absolute Sicherheit für das Verfahrens. Nach derzeitigem Stand der Technik ist der erzeugte Chiffretext nicht brechbar

„one-time-chain“

Der zu verschlüsselnde Text wird in gleicher Länge mit einem aus der CypherMatrix entnommenen Schlüssel **XOR**-verknüpft. Das Ergebnis als Bit-folge holt mit den dezimalen Werten der Elemente aus dem gewählten Zeichen satz das zugeordnete Zeichen und verbindet es zur Bit-Konversion .

Da Klartext und Schlüssel immer die gleiche Länge haben, entsteht ein „**partielles one-time.pad**“. Der Schlüssel wird auch nicht wiederholt. In jeder Runde wird ein anderer Schlüssel aus der jeweiligen CypherMatrix entnommen. Das ergibt für den gesamten Vorgang eine Kette zusammenhängender „one-time-pad“ Funktionen, gewissermaßen als eine „**one-time-chain“**.

Bit-Konversion

Bisher werden Umwandlungen von Bitgfolgen nur im Verfahren „Coding Base64“ vorgenommen [#3], indem 8-bit Sequenzen in eine Folge von 6-bit Sequenzen umgewandelt werden. Die dezimalen Werte dieser Sequenzen sind Indizes für ein statisches Chiffre-Alphabet von 64 Zeichen.

Die **Bit-Konversion** wandelt 8-bit Sequenzen in 7-bit Elemente um. Dabei bleiben die Anzahl der Bits und ihre Reihenfolge gleich. Kein Bit wird hinzu-gefügt und kein Bit wird weggelassen. Nur die Anzahl der Bits in einer Einheit ändert sich. Die dezimalen Werte der neuen Einheiten sind Indexwerte für das zugeordnete Runden-Alphabet. Die Bit-Konversion (Basis 8 zur Basis 7) geschieht im Einzelnen wie folgt:

Bitfolge vor Umwandlung:

011000100110100101110100011001100110111101101100011100

98 105 116 102 111 108

Bitfolge nach Konversion:

011000100110100101110100011001100110111101101100011100

49 26 46 70 51 61 88

Der im gewählten Zeichensatz generierte Chiffretext wird in einer Datei mit dem Namen der Originalfassung und dem Zusatz >**ctx**< gespeichert und steht zur weiteren Verwendung zur Verfügung.

original.txt.ctx -----> Empfänger

Entschlüsselung

Die Entschlüsselung wird im Codierbereich abgearbeitet, nur in der umgekehrten Reihenfolge:

1. Analyse des Chiffretextes
   Chiffretext → Runden-Alphabet (0...256) → 8-bit XOR-Verknüpfung
2. XOR-Verknüpfung
   8-bit XOR-Verknüpfung → Blockschlüssel → Klartext-Block

Aus Blöcken von 64 Zeichen Chiffretext sucht das Verfahren im identisch erzeugten Runden-Alphabet die dezimalen Index-Werte der einzelnen Zeichen und erzeugt mit dem Index aus dem gewählten Zeichensatz die XOR-Folge, die wiederum mit dem Blockschlüssel verknüpft, den Klartext ergibt..

Beispiel Demo-Programm

Das folgende Beispiel läuft unter >Python 3.7.2 / IDLE / run<.
Mit Programm „**CypherMatrix-Demo.py**" verschlüsselte Datei „**info13.txt**" zeigt den folgenden Datenverlauf:

```
>CypherMatrix-Demo<
Verschlüsselungsprogramm
(CypherMatrix-Verfahren)

Auswahl:          Transfer   ..E..  (europäisch)
                             ..R..  (kyrillisch)
                             ..J..   (japanisch)
                             ..C..  (chinesisch)
                             ..K..  (koreanisch)
                             ..I..   (indisch, bengalisch)
                             ..V..   (verschieden)

                             ..q..   (beenden)
Bereich wählen > E
                    Zeichensatz:  Europäisch: E1/19/03/19

ǩOQ̃DZØè½Ə×ÎtaÕhjêɬVÐ+ƌæƯ=Æ Ŭo?
iƴFǑ©Ğ℔NъÑY@ĭơβgÔŊÅƐȵYRmdkÖJ5lpÆzÍğ®èeƒúÀŭDzƮxXÉƀü(Ɵ℗ÝŏǰMP,njÀÂŬ₂U|
ȝ℩ǫSqÁ>ÙBNJwlãĭøvÓàĂ6ƈKÊ€DɣÂ:îÇÌçȝǨ0ÛÅ¾;ƶɳØÜåòŭƠ]ÚCTcƤÈƁ-
bƆÒLÚȝĆHƐəyΣÆHʊƙKdz<áæÔùhʊâà4Î2äÃÄơ7ƦrƱÞgÐÙ${ĆţGƎÏǫ
%ƶæãǫÈsE8¿ZöâШßŘƱlj*3&ÃÁũƱƠ9ÎŨ)WTInfƊfƇÊQuƀđ1Ë.AÒÑåô!ãÌ¶ЄД
 Umfang:  256  Zeichen

 Eingabe der Startphrase: Schwarze Raben auf roten Felsen in der goldenen
Abendsonne
 Startphrase:  Schwarze Raben auf roten Felsen in der goldenen Abendsonne
 Umfang:  58  Zeichen

 Bereich wählen:     verschlüsseln  ..v.. / entschlüsseln  ..e.. /  beenden ..q.. >  v
```

Verschlüsselung der Test-Datei:

Eingabe der Test-Datei: info13.txt

['VERTRAULICH: Am Donnerstag 27.Mai 2019 findet im Freisinger Hof München ein geheimes Treffen der blauen Dragoner statt. Die Dragoner mögen die Öffentlichkeit nicht, daher ist\n', 'größte Umsicht geboten. Bitte, Teilnehmer und Themen ermitteln.\n']

Klartext-Block 1 (Länge: 56 Zeichen)

Matrix-Schlüssel 1
ÝSB€ʅĂÂĀɣ℗ʅǫĀǿɣʅK>ɣĂvƈĀǿɣǘĀă6ĀǿɣNJǿɣqĀĂɣÙvăqĀǿĀǿɣğǫĀǿq6vǿǿĀ
Umfang: 58 Zeichen

Trennkonstante: 3249

Cypherfolge (Ziffern Base 77):

iPζQkVNBkT7gVEξyMNθKKβ9Blhkγe2EWAekg4edhGVδ2awTκ13lıE3ΩεUXvZl115OYı1wβ
Bi9a8DΩβξLJ3cbyunf2FnRJλ2fNJVNML2μr7DS6eJGcUPJOcXmɑVee5nUVh62pΩFWpξew
WλFdz39F3AI9ceX4prW3zVGIwneGμq3jT4Rm8ZkZdxwWDBv3MımDΩAdNoKLWG4e7T
mQΩcc0ıow84AchεκY2Egɑ4IFQfpxTOmbeOyl4YvUec5ıq2ηδBo55FηwwUhκ5u9mt1εC2p
FngyaMEPV5te00gıEvax3ζJ6BMvGpγPraEɑCλ76sV6uκzo2εui66dGyeδzcv9qξIv7fs6GtAx
GayζZo7ξYDq2δ6Q9uγZr7NXVmratr8sμBVλFKβηBvDV9βX8GNwκMMκwNG8Xβ9VDvBηβ
KFλVBμs8rtarmVXN7rZγu9Q6δ2qDYξ7oZζyaGxAtG6sf7vIξq9vczδeyGd66iuε2ozκu6Vs6
7λCɑEarPγpGvMB6Jζ3xavEıg00et5VPEMaygnFp2Cε1tm9u5κhUwwηF55oBδη2qı5ceUvY
4lyOebmOTxpfQFI4ɑgE2YκεhcA48woı0ccΩQmT7e4GWLKoNdAΩDmıM3vBDWwxdZkZ8
mR4Tj3qμGenwIGVz3Wrp4Xec9IA3F93zdFλWweξpWFΩp26hVUn5eeVɑmXcOJPUcGJe6
SD7rμ2LMNVJNf2λJRnF2fnuybc3JLξβΩD8a9iBβw1ıYO511lZvXUεΩ3EıI31κTwa2δVGhde4
gkeAWE2eγkhlB9βKKθNMyξEVg7TkBNVkQζPiδa
Länge: 798 Ziffern (Base 77/78)

alpha: 52
beta : 24
gamma: 101
theta: 29

CypherMatrix
Bh63®ÅƃpäƱu℗Ǩ+GţvÝ×ǽȦàôǑÚ½ÌÅÂǴƐǛ
ăÈĐ;Ç¶Ŭd9xT(ƵỆ©Æ¾âəĐÑØÔkǢĂÉi%ÓyDZ
dzRɣơEaQYǾʓZǗƎç¿ꝚȀnjȻĨŊNÖÊȡ*mâɤKjÔá
ƈȁƂ@FɪthƲƜȣȐ|ǰ!4ȈǭŏI{ƊêǣƢȥȍTÄṅÏ:l
ŭljǘǼPNǟLãåUDùJÃËηæÎȋ ƐƆ8ğǞDz?ǫeü,
$ưƧǘÀHÒȉqƩƖÁrȄƒƤȡ<ǯA€ϴfKъfӇ>NJ1ÞǛ
)ÎÙƨgWД-SǖƠǻƥЪwo&ƓÂßXǿ5ƯzCƏƍ=ǸǬs
VǕĭÜöbɄ0ơ.ǡłOʅcèMΣÕǩȅǦYÍȚÛ7ǫ3ƲnȌ
Umfang: 256 Zeichen

Runden-Alphabet
ÑØÔkǢĂÉi%ÓyDZdzRɣơEaQYǾʓZǗƎç¿ꝚȀnjȻĨ
ŊNÖÊȡ*mâɤKjÔáƈȁƂ@FɪthƲƜȣȐ|ǰ!4ȈǭŏI{
ƊêǣƢȥȍTÄṅÏ:lŭljǘǼPNǟLãåUDùJÃËηæÎȋ
ƐƆ8ğǞDz?ǫeü,$ưƧǘÀHÒȉqƩƖÁrȄƒƤȡ<ǯA
Umfang: 128 Zeichen

Klartext Block: 1
['VERTRAULICH: Am Donnerstag 27.Mai 2019 findet im Freis
Umfang: 56 Zeichen

Runden-Schlüssel 1
Ú½ÌÅÂǴƐǛăÈĐ;Ç¶Ǔd9xT(ƵÊ©Æ¾âəĐÑØÔkǢǍÉi%ÓyDZdzRƳƍEaQYǾǯZŰƎç¿Ʀ
Umfang: 56 Zeichen

XOR --> one-time-pad: 1
{FǣǴĬƃùДÖǉÂÏR%îÊȍlßzKǼǘZȌdzǴ3×ÞǯƯ6+ǦzAÍCJƶÝDzljǣǿLȈȉȡȡæƍǛrƍ
Umfang: 56 Zeichen

Chiffretext (8-bit --> 7-bit): 1
ĬÁ:LÁJãLÑiƶƒÖ,ǾǰêƆƃ!ÖáÑJȉƻm : ȡmƤNdzIǔƕJË ÔDƖǮǯHƈËÓüJDZŰưQikTǧǼǯdzƜ
Umfang: 64 Zeichen

Klartext-Block 2 (Länge: 56 Zeichen)

Matrix-Schlüssel 2
iƕƜ℅Ȑ|ǰ!4ȈǭǒI{ƊêǣƢƶȍTÄǹÏ:IǔǉǘǼPNāLãåUDùJÃËηæȊî ƐƆ8ǧǠDz?ǫ
Umfang: 56 Zeichen

Trennkonstante: 3025

Cypherfolge (Ziffern Base 77):

nMJQLeDXFMuc8okFbEκDδlvLH10βkoTαCSxsWrpcbomDdDdubpFNabQJhsιγTB1κzM4bε
ekRμpP0uNζpY1zζζgue1δαitμf8wBAYδuamZXζδιAK1fDi3SNδlFιvTuλ2ηMQqμsE1mCbon2
θTΩmLιeNsr4gL2CYLqμR0lXc4DoAξIABγ7Rtsn8γVPbLξIOcSθ124ηWaQM8gLXN6X434R
8TEmNUlHNv31ξμJdGM08fOvV38ON5CδtβYZ0Ci411NξvvIOwqtiC514Aξ8YTAt0zuη43pn
h8j9βsuZdW235Bv72TmOQbNi51HΩW2αθgKLKθD27tVJvYuawε3mfS1c9qjvvJNED1eq1
ηJεYp33vκ76i17NmΩyoUγgn96F66κwKfmmfKwκ66F69ngγUoγΩmN71i67κv33pYεJη1qe
1DENJvvjq9c1Sfm3εwauYvJVt72DθKLKgθα2WΩH15iNbQOmT27vB532WdZusβ9j8hnp3
4ηuz0tATY8ξA415CitqwOIvvξN114iC0ZYβtδC5NO83VvOf80MGdJμξ13vNHlUNmET8R43
4X6NXLg8MQaWη421θScOIξLbPVγ8nstR7γBAIξAoD4cXl0RμqLYC2Lg4rsNeιLmΩTθ2nob
Cm1EsμqQMη2λuTvιFlδNS3iDf1KAιδζXZmauδYABw8fμtiαδ1eugζζz1YpζNu0PpμRkeεb4M
zκ1BTγιshJQbaNFpbudDdDmobcprWsxSCαTokβ01HLvlδDκEbFko8cuMFXDeLQJMn92
Länge: 764 Ziffern (Base 77/78)

alpha: 23
beta : 40
gamma: 144
theta: 11

CypherMatrix

ÊƗQI©äƩucǰFÎBǔânj3iƈ{ЪVPjÂÕǣƍƟţƢ>
ȉƷNJǒáƇǺzȌɄØƬÊƖĭ+¾*ăǢ=ÜъД℅OXvƂÖ€W
ǟÏ,əôǬĐǽ.Ʊtƍ@aÔK;ÓƏǠȗú$ÙĂƊnÞeh8Å
ƦüƐxƓȉưàg%ÉƶyNǼ0ã&ÔDzƎ ƐƒL<ǫɓmǻiǭ
℗ȘȡÀ½ǚ7TǧA|ƕꞪȀ×q?ǕǓÄÁǨp6ƪȁæUƳǯηd
êîǛÑ-ZΣGƯÚDZȆCƱƨ9J4YƤgw(ȍåσß®f!ǡɣ
ƵÍǾkĐŰǮÛȒdzǦƆçÂƜ1ljöÝƒÇâǹǿDĬèKÈ5ȅË
YoȡǞǙŊǑü¿¶MHǸÎs:)IbǩβRƮÒÆƧÃrǴEƠÌ
Umfang: 256 Zeichen

Runden-Alphabet
jÂÕæɋΘţƠ]>ì3NJǒáĆÅzÒЎØTÊlĭ+¾*ăÆ=Üъ
ДꞨOXvБÖ€WãÏ,əôǪÐǽ.Ʊtơ]@aÔK;ÓƏĀūú$
ÙĂĎnÞeh8ÅĸüɛxĜÌưàg%ÉƶyNÆ0ã&ÔDzƎ ɛ
ƒL<ǫƀmåiǫ℗SƌÀ½ǔ7TğA|ʰƲÀ×q?ŨŮÄǍǩp
Umfang: 128 Zeichen

Klartext Block: 2
inger Hof München ein geheimes Treffen der blauen Dragon
Umfang: 56 Zeichen

Runden-Schlüssel 2
ÒЎØTÊlĭ+¾*ăÆ=ÜъДꞨOXvБÖ€WãÏ,əôǪÐǽ.Ʊtơ]@aÔK;ÓƏĀūú$ÙĂĎnÞeh8Å
Umfang: 56 Zeichen

XOR --> one-time-pad: 2
ɛШQÛɛ?SîŨôFţɣfüLxFY½ǎ ŧǯΣəÅsǯàƐğ;Ʊă¿üÃêVŨǪъƏƨъāǪ?ǎùæꞨwəƊ
Umfang: 56 Zeichen

Chiffretext (8-bit --> 7-bit): 2
ǽƷ<ĭǫæ8ǼĂ8j½ğÀǒl0¾aĠÀÔAɋ|Ə7ƲSpÆƱ.ǫãÔ|mNJØĭÀØÐƠ]K;ÁÀúÌƎĂǼŮǫ*ƶǻ½ƶyúÊ
Umfang: 64 Zeichen

(im Folgenden werden nur der Klartext und der Chiffretext gezeigt)

Klartext-Block 3 (Länge: 56 Zeichen)

Klartext Block: 3
er statt. Die Dragoner mögen die Öffentlichkeit nicht, d
Umfang: 56 Zeichen

Chiffretext (8-bit --> 7-bit): 3
YơUaǻÎÎ;½ƎæƈΣţŮ!ÃŢơÑ|¿ДƯ½Σ6+Ɛ.ţъƨ:7äÎKCfɣÎr&ÉgŘH!ŏêƵyGa>ÀÀ.5&Ñ!Ţ
Umfang: 64 Zeichen

Klartext-Block 4 (Länge: 56 Zeichen)

Klartext Block: 4
aher ist\n', 'größte Umsicht geboten. Bitte, Teilnehmer
Umfang: 56 Zeichen

Chiffretext (8-bit --> 7-bit): 4
Ï+ÔküpâYĆ+ƉÅ-½PkÔÜШţeơǝÞeáÏƉ¿fШ+¾¾üPƶÐwÜ%ÝÜßòljÖi,Ãzf9ƱXΣzƤ%ÞǪxƶǪ
Umfang: 64 Zeichen

Klartext-Block 5 (Länge: 56 Zeichen)

Klartext Block: 5
und Themen ermitteln.\n']
Umfang: 25 Zeichen

Chiffretext (8-bit --> 7-bit): 5
ŰÊƁ%ŭƶŮvƠ]àcƎɳfÆGƆcZĆǩ=;VTTƐĀ
Umfang: 28 Zeichen

Chiffretext an den Empfänger: info13.txt.ctx

ĬÁ:LÁJãLÑizƒÖ,ǾĵêƆƃ!ÖáÑJ̀ì2m : ƋmƤNdzIŭƕJË
ÔDƖǯʒHƇËÓüJDZŰưQikƬğǼʒdzƜǽ3<ĭọǣ8ǢĂ8j½ğȀŏl0¾aƓȀÔAȩ|Ә7ҤSpǢƱ.ọãÔ|
mNJØĭÀØĐƆ|K;ÁÀűȉƎĂǼŬọ*ƶǻ½ƶyűÊYơUaǻÎȊ;½ƎǣƇΣţŬ!ÃƮơÑ|
¿ДƯ½Σ6+Ɛ.ţъƧ:7äÎKCƒƔÎr&ÉgȐH!ŏêƵyGa>ǸÀ.5&Ñ!ƮÏ+ÔküpâYǴ+ƊÅ-
½PkȎÜƜţeơȇÞeáÏƊ¿fƜ+¾¾üPƶĐwÜ%ÝÜßòljǑi,ÃzƒƐ9ƱXΣzƤ%ÞǬxƶǬǗÊƃ
%ŭƵǓvƆ|àcƎƞfǢGƆcZǴǩ=;VTƬƐǠ

Der Chiffretext ist gespeichert in der Datei: info13.txt.ctx

Das Programm ist beendet

Um selbst zu testen, kann das Verfahren im Internet unter telecypher.net/CypherMatrix-Algorithmus.zip aufgerufen werden. Für weitere Erläuterungen steht Ihnen der Autor eschnoor@multi-matrix.de jederzeit zur Verfügung.

München, den 30.Mai 2019

[#1] telecypher.net/Neue Funktionen in der Kryptographie.pdf
[#2] wikipedia.org/One-Time-Pad
[#3] wikipedia.org/wiki/Base64